ABSTRACT

A method for determining a result of a group operation performed an integral number of times on a selected element of the group, the method comprises the steps of :representing the integral number as a binary vector; initializing an intermediate element to the group identity element; selecting successive bits, beginning with a left most bit, of the vector. For each of the selected bits; performing the group operation on the intermediate element to derive a new intermediate element; replacing the intermediate element with the new intermediate element; performing the group operation on the intermediate element and an element, selected from the group consisting of: the group element if the selected bit is a one; and an inverse element of the group element if the selected bit is a zero; replacing the intermediate element with the new intermediate element. In a final step, performing the group operation on the intermediate value and the inverse element if the last selected bit is a zero; and replacing the intermediate element therewith, to obtain the result, whereby each of the bits of the integral is processed with substantially equal operations thereby minimizing timing attacks on the cryptographic system.